セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」

小野寺 久人　好本 雅道　山本 和也

要 旨

企業や公的機関などの情報システムをターゲットにしたサイバー攻撃による被害が社会的な問題になっています。高度化する攻撃に対抗するには、複数の対策を組み合わせた多層防御が必要です。多層防御は、事前対策、脅威検知、事後対策から構成されます。事前対策である脆弱性管理は、機器の構成情報の把握、脆弱性情報の把握、脆弱性の調査・リスク分析、対策の実施というステップで行います。これらのステップにおける問題を説明し、NECで利用しているソリューション「NEC Cyber Security Platform」を紹介します。

KeyWords　数えるマネジメント／見える化／サイバー攻撃／事前対策／脆弱性管理

1. はじめに

昨今、企業や公的機関などの情報システムをターゲットとするサイバー攻撃が増加するとともに、従来は個人の愉快犯が中心であったものが、プロの犯罪者によるビジネスへと変化しています。社外に公開するサーバが不正アクセスを受け、数百万件の顧客情報が流出した事案や、海外の重要インフラ企業のワークステーション数万台がウイルスに感染し内部システムのネットワーク遮断が発生した事案など、サイバー攻撃による被害は後を絶ちません。

本稿では、サイバー攻撃に対するNECの考え方、対策について紹介します。

2. サイバー攻撃対策

高度化する攻撃に対抗するには複数の対策を組み合わせた多層防御による対策が必要です。多層防御では1つの対策が破られても次の対策で攻撃を防ぐという考えに基づいています。多層防御を構成する個々の技術的対策は大きく分けて「事前対策」「脅威検知」「事後対策」に分けられます。

(1) 事前対策

事前対策は、攻撃が行われた場合の侵入を未然に防ぐための予防策です。脆弱性情報を収集してセキュリティパッチを機器に適用すること、管理者権限を必要最小限のユーザーのみに限定することで権限のないユーザーが重要情報にアクセスできないように制限を実施すること、許可されたアプリケーションのみを利用可能にするアプリケーションのホワイトリスト化などが挙げられます。

(2) 脅威検知

脅威検知は、事前対策で防げず、侵入された脅威を見つけることです。サーバや端末、ネットワーク機器などのログや各種セキュリティ製品のアラートを集約して、不審な通信が発生していないか、管理者ユーザーのログイン失敗が大量に発生していないかなどを調べることでマルウェアの侵入や攻撃の成功を検知します。一般的には、セキュリティオペレーションセンターと呼ばれる専門組織が担当します。

(3) 事後対策

事後対策は、攻撃を受けた後の被害を極小化することです。まず、影響範囲を特定し、端末隔離やパスワード変更などの暫定対処を実施して被害の拡大を防止します。次に、フォレンジックやマルウェア解析などの本格対処を行うことで被害全貌を把握したうえで、

汚染された機器のクリアインストールなどを行い復旧します。情報流出が確認された場合や、自社が提供するサービスに影響が出た場合など、必要に応じて社外へ報告や情報公開を行います。

3. 事前対策の効果とNECの脆弱性管理

オーストラリア電信電子局（Australian Signals Directorate:ASD）が提唱する“Strategies to Mitigate Cyber Security Incidents”[1]によると、事前対策である「アプリケーションの利用制限（ホワイトリスト化）」「アプリケーションを最新の状態に保持（セキュリティパッチ適用）」「管理者権限の最小化」を実施することで、85%のサイバー攻撃が防御可能と試算されています。

実例として、2017年5月に世界150カ国、30万台以上の機器に感染したランサムウェアWannaCry[2]は、2017年3月にパッチが公開されているCVE-2017-0145の脆弱性を悪用しています[3]。そのため、セキュリティパッチの適用ができていれば被害は発生しませんでした。

ASDが提唱する対策のうちセキュリティパッチ適用は、導入コストやメンテナンスコストが高いと評価されており、導入・運用は難しいと考えられています。一方で、NECではサイバー攻撃から社内の情報インフラ、情報資産を守るため2002年からサイバー攻撃防御システム（Cyber Attack Protection System:CAPS）を開発し、社内のパッチ適用を社内18万台に対して実践し、アプリケーションを最新の状態に保持してきました。CAPSでは「数えられるものが管理できる」という「数えるマネジメント」の考え方に従って、機器がどこに何台あるのか、そのうち対策が必要な機器が何台あるのかを数えることでリスクを可視化し、脆弱性を管理しています。これにより攻撃そのものは防げなくとも、攻撃により被害に遭うリスクの大幅な低減に成功しています。以降の章では脆弱性管理に絞って解説します。

4. 脆弱性管理の手順と問題

一般に脆弱性管理は以下の手順で行われます[4]。

（1）構成情報の把握
（2）脆弱性情報の把握
（3）脆弱性の調査・リスク分析
（4）対策の実施

各手順の考え方と実施プロセスでの問題を説明します。

（1）構成情報の把握

社内の機器の総数把握と機器ごとのソフトウェア構成情報を収集し、管理を行うことです。構成情報を収集することで脆弱性が発見されたときの対処を迅速に行うことができます。

このプロセスでの問題は、管理対象機器が多数存在するため、保有する機器の使用ソフトウェア、及びそのバージョンの把握が十分にできないことです。

（2）脆弱性情報の把握

各OS、ソフトウェアベンダーのWebサイトやIPA、JPCERT/CCなどの脆弱性情報を発信している組織から公開される脆弱性情報を日々収集します。社内システムの構成情報と入手した脆弱性情報から必要な情報を精査し、取捨選択します。

このプロセスでの問題は、公開される脆弱性情報やベンダーから提供される大量のパッチ情報から自社に関係あるものがどれかを調べるのに時間がかかることです。

（3）脆弱性の調査・リスク分析

収集した情報からリスクの高い脆弱性を選定し、収集した構成情報と突き合わせることで自社への影響を確認し、対処要否の判断を行うことです。

このプロセスでの問題は、自社への影響調査を実施するにも、各部門への調査依頼や管理台帳と突き合わせに時間がかかり、迅速な対応ができないことです。

（4）対策の実施

対策が必要と判断した脆弱性に対して、パッチ適用や運用回避などの対策を立案し、実行します。セキュリティ管理者は対策の実施状況を監視し、すべての機器で対策が完了したことを確認します。

このプロセスでの問題は、対策を人手で実施するには膨大なコストがかかることです。例えば1万台の機器に対して脆弱性が100個ある場合、100万件の対策実行と結果確認が必要となり、人手で確認するのは困難です。また、部門間のコミュニケーションミスにより、実態を確認できない場合もあります。

5.「NEC Cyber Security Platform」

先に述べたとおりNECでは脆弱性管理を行うために

CAPSを運用してきました。2016年度からはCAPSを更新する形でGCAPS（Global Cyber Attack Protection System）をNECグループ全社に対して展開しています。GCAPSのNEC社内での運用実績をもとに「NEC Cyber Security Platform」（以下、NCSP）を製品化しています。

5.1 NCSPの機能とシステム構成

NCSPは社内の機器の脆弱性対策状況の可視化から対策実行までを支援するソリューションであり、次のコンポーネントから構成されています。

（1）NECセキュリティインテリジェンス
（2）NCSPエージェント
（3）NCSPマネージャー

システム構成を**図1**に示します。

5.2 NECセキュリティインテリジェンス

NECセキュリティインテリジェンス（以下、インテリジェンス）は脆弱性情報の把握を支援します。

インテリジェンスはNCSPが脆弱性を調査するための検索式や対策（パッチ、回避策など）の情報が含まれており、脆弱性情報が公開されるたびにNECが情報を収集し、内容を評価して配信します。このインテリジェンスを活用することで、高度なセキュリティスキルがなくてもNECと同様の脆弱性管理が可能となります。

5.3 NCSPエージェント

NCSPエージェントはNCSPマネージャーと連携し、構成情報の把握、脆弱性の調査、対策を実施します。人手を介することがなくなるために、迅速かつコストをかけずに以下のプロセスを実行できます。

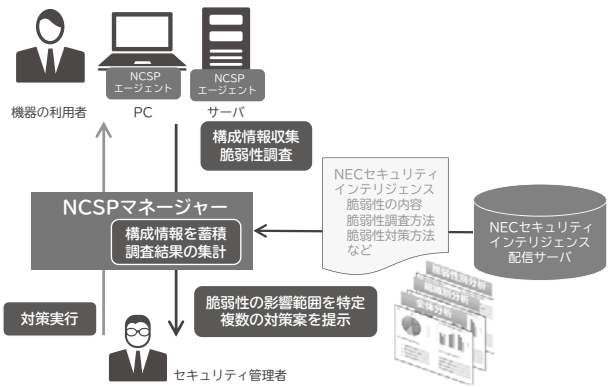


図1　NCSPのシステム構成

図2　リスクビューア（左：一覧画面、右：詳細画面）

図3　NCSPのダッシュボード画面

（1）構成情報の把握

機器の情報（ホスト名、OS名、CPU名、IPアドレス、MACアドレス、インストールされているソフトウェアなど）を自動収集します。

（2）脆弱性の調査

脆弱性を調査するための検索式をNCSPマネージャーから受信し、インストールされているソフトウェアのバージョン、ファイル、レジストリなどを確認することで脆弱性の有無を調査します。また、その結果をNCSPマネージャーへ送信します。

（3）対策の実施

NCSPマネージャーから自動対策の指示を受信した場合には、自動的に対策を適用します。また、手動での対策指示を受信した場合には、**図2**に示すリスクビューアを表示し、機器の利用者へ対策実施を促します。

5.4 NCSPマネージャー

NCSPマネージャーはNCSPエージェントが集めた構成情報や調査結果を組織ごとに集計し、リスクを見える化

します。**図3**にNCSPのダッシュボード画面を示します。

機器全体のリスク状況、脆弱性別・組織別・端末の種類別のリスクがある機器を数えることで、セキュリティ管理者の対策立案を支援します。セキュリティ管理者は脆弱性の内容や機器の種別などを考慮して、対策を指示・実行することができます。

6. おわりに

本稿では、サイバー攻撃とその対策における脆弱性管理の重要性、そのソリューションであるNCSPの紹介をしました。今後はCSIRTの運用を支援するインシデントレスポンス機能を強化していく予定です。

*Apache Struts は、Apache Software Foundation の登録商標または商標です。
*その他記述された社名、製品名などは、該当する各社の商標または登録商標です。

参考文献

1) Australian Signals Directorate：Strategies to Mitigate Cyber Security Incidents
https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
2) The White House：Press Daily Briefing by Press Secretary Sean Spicer -- #48, 2017.5.15
https://www.whitehouse.gov/the-press-office/2017/05/15/press-daily-briefing-press-secretary-sean-spicer-48
3) JPCERT/CC：ランサムウエア"WannaCrypt"に関する注意喚起, 2017.5
https://www.jpcert.or.jp/at/2017/at170020.html
4) 独立行政法人 情報処理推進機構：セキュリティ担当者のための脆弱性対応ガイド～企業情報システムの脆弱性対策～, 2017.3
http://www.ipa.go.jp/files/000011568.pdf

関連URL

NEC Cyber Security Platform
http://jpn.nec.com/ncsp/

執筆者プロフィール

小野寺 久人
スマートネットワーク事業部
主任

好本 雅道
スマートネットワーク事業部
マネージャー

山本 和也
スマートネットワーク事業部

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

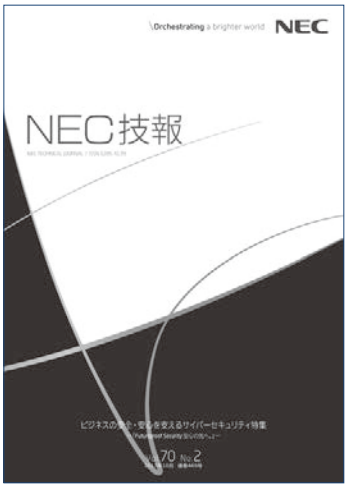
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP